BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平11－175726

(43)公開日　平成11年(1999)７月２日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｔ　7/00		Ｇ０６Ｆ　15/62	４６０
			４６５Ｋ

審査請求　未請求　請求項の数15　ＯＬ　（全９頁）

(21)出願番号　特願平9－342494

(22)出願日　平成９年(1997)12月12日

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(72)発明者　板橋　達夫
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　但野　拓志
東京都品川区北品川６丁目７番35号　ソニー株式会社内

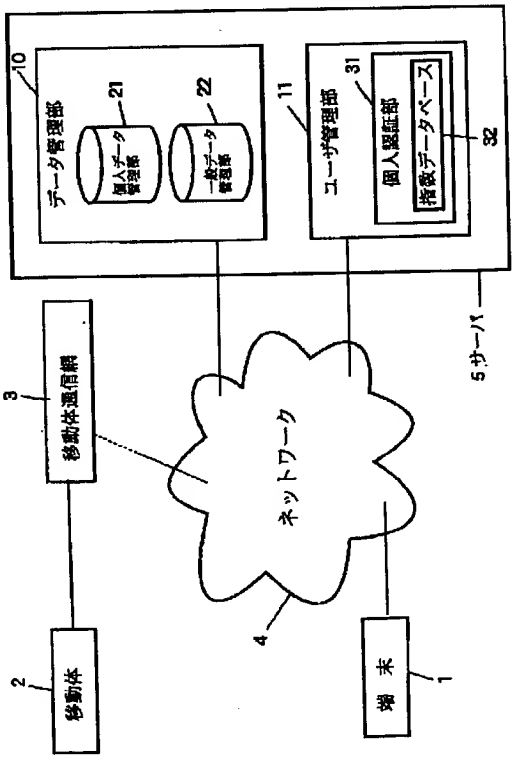
(74)代理人　弁理士　稲本　義雄

(54)【発明の名称】　情報処理装置および方法、情報処理システム、並びに提供媒体

(57)【要約】

【課題】　個人認証後の個人データの取得を簡便化する。

【解決手段】　端末１には、指紋認識装置が備えられている。ユーザは、端末１を用いて個人データを読み出したい場合、指紋認識装置に自分の指紋を入力する。入力された指紋データは、ネットワーク４を介してサーバ５のユーザ管理部１１に伝送される。ユーザ管理部１１の個人認証部３１は、指紋データベース３２に、伝送された指紋データが存在するか否かを判断する。一致する指紋データが存在すると判断された場合、正規のユーザと認証され、データ管理部１０の個人データ管理部２１にアクセスし、保存されているそのユーザ個有のデータを読み出すことが可能となる。



1

【特許請求の範囲】

【請求項１】　個人認証用データを入力する入力手段と、
情報を表示する表示手段と、
前記表示手段に表示された情報を選択する選択手段とを備えることを特徴とする情報処理装置。

【請求項２】　音声の入出力を行う音声入出力手段をさらに備えることを特徴とする請求項１に記載の情報処理装置。

【請求項３】　前記個人認証用データは、指紋であることを特徴とする請求項１に記載の情報処理装置。

【請求項４】　前記個人認証用データは、虹彩であることを特徴とする請求項１に記載の情報処理装置。

【請求項５】　前記個人認証用データは、顔の輪郭であることを特徴とする請求項１に記載の情報処理装置。

【請求項６】　前記個人認証用データは、個人認証用カードに記録されているデータであることを特徴とする請求項１に記載の情報処理装置。

【請求項７】　前記個人認証用データは、手書きサインであることを特徴とする請求項１に記載の情報処理装置。

【請求項８】　個人認証用データを入力する入力ステップと、
情報を表示する表示ステップと、
前記表示ステップで表示された情報を選択する選択ステップとを備えることを特徴とする情報処理方法。

【請求項９】　個人認証用データを入力する入力ステップと、
情報を表示する表示ステップと、
前記表示ステップで表示された情報を選択する選択ステップとを備えるコンピュータプログラムを提供することを特徴とする提供媒体。

【請求項１０】　個人を認証するためのデータを蓄積する個人認証データ蓄積手段と、
他の情報処理装置から送信された個人認証用データが、前記個人認証データ蓄積手段により蓄積されているデータ内に存在するか否かを判断する判断手段と、前記判断手段により個人認証用データが存在していると判断された場合、アクセス可能となる個人データを蓄積する個人データ蓄積手段とを備えることを特徴とする情報処理装置。

【請求項１１】　個人を認証するためのデータを蓄積する個人認証データ蓄積ステップと、
他の情報処理装置から送信された個人認証用データが、前記個人認証データ蓄積ステップで蓄積されたデータ内に存在するか否かを判断する判断ステップと、
前記判断ステップにより個人認証用データが存在していると判断された場合、アクセス可能となる個人データを蓄積する個人データ蓄積ステップとを備えることを特徴とする情報処理方法。

2

【請求項１２】　個人を認証するためのデータを蓄積する個人認証データ蓄積ステップと、
他の情報処理装置から送信された個人認証用データが、前記個人認証データ蓄積ステップで蓄積されたデータ内に存在するか否かを判断する判断ステップと、
前記判断ステップにより個人認証用データが存在していると判断された場合、アクセス可能となる個人データを蓄積する個人データ蓄積ステップとを備えるコンピュータプログラムを提供することを特徴とする提供媒体。

【請求項１３】　第１の情報処理装置と第２の情報処理装置から構成される情報処理システムにおいて、
前記第１の情報処理装置は、
個人認証用データを入力する入力手段と、
前記入力手段に入力された個人認証用データを送信する第１の送信手段と、
情報を表示する表示手段と、
前記表示手段に表示された情報を選択する選択手段とを備え、
前記第２の情報処理装置は、
個人を認証するためのデータを蓄積する個人認証データ蓄積手段と、
前記第１の送信手段により送信された個人認証用データが、前記個人認証データ蓄積手段により蓄積されているデータ内に存在するか否かを判断する判断手段と、
前記判断手段により個人認証用データが存在していると判断された場合、アクセス可能となる個人データを蓄積する個人データ蓄積手段と、
前記個人データ蓄積手段に蓄積されているデータを、前記第１の情報処理装置に送信する第２の送信手段とを備えることを特徴とする情報処理システム。

【請求項１４】　第１の情報処理装置と第２の情報処理装置から構成される情報処理システムの情報処理方法において、
前記第１の情報処理装置は、
個人認証用データを入力する入力ステップと、
前記入力ステップで入力された個人認証用データを送信する第１の送信ステップと、
情報を表示する表示ステップと、
前記表示ステップで表示された情報を選択する選択ステップとを備え、
前記第２の情報処理装置は、
個人を認証するためのデータを蓄積する個人認証データ蓄積ステップと、
前記第１の送信ステップにより送信された個人認証用データが、前記個人認証データ蓄積ステップで蓄積されたデータ内に存在するか否かを判断する判断ステップと、
前記判断ステップにより個人認証用データが存在していると判断された場合、アクセス可能となる個人データを蓄積する個人データ蓄積ステップと、
前記個人データ蓄積ステップで蓄積されたデータを、前

記第１の情報処理装置に送信する第２の送信ステップとを備えることを特徴とする情報処理方法。

【請求項１５】　第１の情報処理装置と第２の情報処理装置から構成される情報処理システムに用いられるコンピュータプログラムであって、

前記第１の情報処理装置のコンピュータプログラムは、

個人認証用データを入力する入力ステップと、

前記入力ステップで入力された個人認証用データを送信する第１の送信ステップと、

情報を表示する表示ステップと、

前記表示ステップで表示された情報を選択する選択ステップとを備え、

前記第２の情報処理装置のコンピュータプログラムは、

個人を認証するためのデータを蓄積する個人認証データ蓄積ステップと、

前記第１の送信ステップで送信された個人認証用データが、前記個人認識データ蓄積ステップで蓄積されたデータ内に存在するか否かを判断する判断ステップと、

前記判断ステップで個人認証用データが存在していると判断された場合、アクセス可能となる個人データを蓄積する個人データ蓄積ステップと、

前記個人データ蓄積ステップで蓄積されたデータを、前記第１の情報処理装置に送信する第２の送信ステップとを備えるコンピュータプログラムを提供することを特徴とする提供媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報処理装置および方法、情報処理システム、並びに提供媒体に関し、特に、個人データを個人認証用データの入力を行うことにより読み出せるようにした情報処理装置および方法、情報処理システム、並びに提供媒体に関する。

【０００２】

【従来の技術】現在、液晶画面が備え付けられた公衆電話がある。この公衆電話の液晶画面には、通信している相手先の電話番号、カードの残量度数などが表示される。また、ISDN（Intergrated Services Digital Network）などのデジタル通信に対応した公衆電話もある。

【０００３】

【発明が解決しようとする課題】しかしながら、上述した公衆電話にユーザを認証し、認証後にそのユーザ個人の情報を、備え付けられている液晶画面に表示させるようなサービスは行われていない。

【０００４】本発明はこのような状況に鑑みてなされたものであり、公衆電話など、多数のユーザが利用する端末において、各ユーザを認証する装置を設け、さらに各ユーザ個人の情報を提供できるようにするものである。

【０００５】

【課題を解決するための手段】請求項１に記載の情報処理装置は、個人認証用データを入力する入力手段と、情報を表示する表示手段と、表示手段に表示された情報を選択する選択手段とを備えることを特徴とする。

【０００６】請求項８に記載の情報処理方法は、個人認証用データを入力する入力ステップと、情報を表示する表示ステップと、表示ステップで表示された情報を選択する選択ステップとを備えることを特徴とする。

【０００７】請求項９に記載の提供媒体は、個人認証用データを入力する入力ステップと、情報を表示する表示ステップと、表示ステップで表示された情報を選択する選択ステップとを備えるコンピュータプログラムを提供することを特徴とする。

【０００８】請求項１０に記載の情報処理装置は、個人を認証するためのデータを蓄積する個人認証データ蓄積手段と、他の情報処理装置から送信された個人認証用データが、個人認証データ蓄積手段により蓄積されているデータ内に存在するか否かを判断する判断手段と、判断手段により個人認証用データが存在していると判断された場合、アクセス可能となる個人データを蓄積する個人データ蓄積手段とを備えることを特徴とする。

【０００９】請求項１１に記載の情報処理方法は、個人を認証するためのデータを蓄積する個人認証データ蓄積ステップと、他の情報処理装置から送信された個人認証用データが、個人認証データ蓄積ステップで蓄積されたデータ内に存在するか否かを判断する判断ステップと、判断ステップにより個人認証用データが存在していると判断された場合、アクセス可能となる個人データを蓄積する個人データ蓄積ステップとを備えることを特徴とする。

【００１０】請求項１２に記載の提供媒体は、個人を認証するためのデータを蓄積する個人認証データ蓄積ステップと、他の情報処理装置から送信された個人認証用データが、個人認証データ蓄積ステップで蓄積されたデータ内に存在するか否かを判断する判断ステップと、判断ステップにより個人認証用データが存在していると判断された場合、アクセス可能となる個人データを蓄積する個人データ蓄積ステップとを備えるコンピュータプログラムを提供することを特徴とする。

【００１１】請求項１３に記載の情報処理システムの第１の情報処理装置は、個人認証用データを入力する入力手段と、入力手段に入力された個人認証用データを送信する第１の送信手段と、情報を表示する表示手段と、表示手段に表示された情報を選択する選択手段とを備え、第２の情報処理装置は、個人を認証するためのデータを蓄積する個人認証データ蓄積手段と、第１の送信手段により送信された個人認証用データが、個人認証データ蓄積手段により蓄積されているデータ内に存在するか否かを判断する判断手段と、判断手段により個人認証用データが存在していると判断された場合、アクセス可能となる個人データを蓄積する個人データ蓄積手段と、個人データ蓄積手段に蓄積されているデータを、第１の情報処

理装置に送信する第２の送信手段とを備えることを特徴とする。

【００１２】請求項１４に記載の情報処理方法は、第１の情報処理装置は、個人認証用データを入力する入力ステップと、入力ステップで入力された個人認証用データを送信する第１の送信ステップと、情報を表示する表示ステップと、表示ステップで表示された情報を選択する選択ステップとを備え、第２の情報処理装置は、個人を認証するためのデータを蓄積する個人認証データ蓄積ステップと、第１の送信ステップにより送信された個人認証用データが、個人認証データ蓄積ステップで蓄積されたデータ内に存在するか否かを判断する判断ステップと、判断ステップにより個人認証用データが存在していると判断された場合、アクセス可能となる個人データを蓄積する個人データ蓄積ステップと、個人データ蓄積ステップで蓄積されたデータを、第１の情報処理装置に送信する第２の送信ステップとを備えることを特徴とする。

【００１３】請求項１５に記載の提供媒体は、第１の情報処理装置のコンピュータプログラムは、個人認証用データを入力する入力ステップと、入力ステップで入力された個人認証用データを送信する第１の送信ステップと、情報を表示する表示ステップと、表示ステップで表示された情報を選択する選択ステップとを備え、第２の情報処理装置のコンピュータプログラムは、個人を認証するためのデータを蓄積する個人認証データ蓄積ステップと、第１の送信ステップで送信された個人認証用データが、個人認識データ蓄積ステップで蓄積されたデータ内に存在するか否かを判断する判断ステップと、判断ステップで個人認証用データが存在していると判断された場合、アクセス可能となる個人データを蓄積する個人データ蓄積ステップと、個人データ蓄積ステップで蓄積されたデータを、第１の情報処理装置に送信する第２の送信ステップとを備えるコンピュータプログラムを提供することを特徴とする。

【００１４】請求項１に記載の情報処理装置、請求項８に記載の情報処理方法、および請求項９に記載の提供媒体においては、個人認証用データが入力され、情報が表示され、表示された情報が選択される。

【００１５】請求項１０に記載の情報処理方法、請求項１１に記載の情報処理方法、および請求項１２に記載の提供媒体においては、個人を認証するためのデータが蓄積され、他の情報処理装置から送信された個人認証用データが、個人認証データ蓄積ステップで蓄積されたデータ内に存在するか否かが判断され、個人認証用データが存在していると判断された場合、アクセス可能となる個人データが蓄積される。

【００１６】請求項１３に記載の情報処理システム、請求項１４に記載の情報処理方法、および請求項１５に記載の提供媒体においては、第１の情報処理装置は、個人認証用データが入力され、入力された個人認証用データが送信され、情報が表示され、表示された情報が選択され、第２の情報処理装置は、個人を認証するためのデータが蓄積され、第１の情報処理装置から送信された個人認証用データが、蓄積されたデータ内に存在するか否かが判断され、個人認証用データが存在していると判断された場合、アクセス可能となる個人データが蓄積され、蓄積されたデータが、第１の情報処理装置に送信される。

【００１７】

【発明の実施の形態】以下に本発明の実施の形態を説明するが、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を付加して本発明の特徴を記述すると、次のようになる。但し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

【００１８】請求項１に記載の情報処理装置は、個人認証用データを入力する入力手段（例えば、図２の指紋認識装置５４）と、情報を表示する表示手段（例えば２のディスプレイ５１）、表示手段に表示された情報を選択する選択手段（例えば、図２の選択ボタン５３）とを備えることを特徴とする。

【００１９】請求項２に記載の情報処理装置は、音声の入出力を行う音声入出力手段（例えば、図２の受話器５２）をさらに備えることを特徴とする。

【００２０】請求項１０に記載の情報処理装置は、個人を認証するためのデータを蓄積する個人認証データ蓄積手段（例えば、図１の指紋データベース３２）と、他の情報処理装置から送信された個人認証用データが、個人認識データ蓄積手段により蓄積されているデータ内に存在するか否かを判断する判断手段（例えば、図１の個人認証部３１）と、判断手段により個人認証用データが存在していると判断された場合、アクセス可能となる個人データを蓄積する個人データ蓄積手段（例えば、図１の個人データ管理部２１）とを備えることを特徴とする。

【００２１】請求項１３に記載の情報処理システムは、第１の情報処理装置は、個人認証用データを入力する入力手段（例えば、図２の指紋認識装置５４）と、入力手段に入力された個人認証用データを送信する第１の送信手段（例えば、図３のステップＳ３）と、情報を表示する表示手段（例えば、図２のディスプレイ５１）と、表示手段に表示された情報を選択する選択手段（例えば、図２の選択ボタン５３）とを備え、第２の情報処理装置は、個人を認証するためのデータを蓄積する個人認証データ蓄積手段（例えば、図１の指紋データベース３２）と、第１の送信手段により送信された個人認証用データが、個人認識データ蓄積手段により蓄積されているデータ内に存在するか否かを判断する判断手段（例えば、図１の個人認証部３１）と、判断手段により個人認証用デ

ータが存在していると判断された場合、アクセス可能となる個人データを蓄積する個人データ蓄積手段（例えば、図１の個人データ管理部２１）と、個人データ蓄積手段に蓄積されているデータを、第１の情報処理装置に送信する第２の送信手段（例えば、図３のステップＳ１０）とを備えることを特徴とする。

【００２２】図１は、本発明の情報処理システムの構成例を示すブロック図である。端末１は、個人認証用データが入力される認証装置（後述）を備えた端末であり、例えばISDN（Intergrated Services Digital Network）によりネットワーク４と接続されている。またネットワーク４には、移動体２（例えば、飛行機、自動車、電車）が、移動体通信網（例えば、衛星）を介して接続されている。さらにネットワーク４は、サーバ５とも接続されている。移動体２には、端末１と同様な処理を行える端末が備え付けられている。

【００２３】サーバ５は、個人ユーザのデータを管理する個人データ管理部２１と、複数のユーザが共用するデータを管理する一般データ管理部２２とから構成されているデータ管理部１０と、ユーザの認証を行うユーザ管理部１１とから構成されている。ユーザ管理部１１は、ユーザを認証するためのデータの管理を行う個人認証部３１から構成されている。個人認証部３１は、例えば、指紋によりユーザの認証を行う場合、ユーザの指紋に関するデータが登録されている指紋データベース３２より構成される。

【００２４】データ管理部１０には、ユーザ管理部１１においてユーザの認証が行われ、正当なユーザであることが確認された後でないと、アクセスすることはできない。

【００２５】個人データ管理部２１には、ユーザの管理する住所録、スケジュール、顧客情報、預金残高など、そのユーザ個有の情報が管理（保存）されている。従って、個人データ管理部２１は、プライバシ保護の観点から、外部に情報が漏れないようにすることが大切であり、そこにアクセスするためには、ユーザ管理部１１によるユーザの認証により正当なユーザであると判断される必要がある。また、個人データ管理部２１にアクセスしてきたユーザに関する履歴は、サーバ５に保存される。

【００２６】一般データ管理部２２は、複数のユーザが共通に使用するプログラムや、データが管理されている。その中には、有料で配布されるデータも管理されている。この情報処理システムにおいては、データを取得する際、必ずユーザ管理部１１において、ユーザの認証が行われ、正規のユーザであると判断された後にデータを取得できる仕組みになされているので、例えば、有料データの料金の徴収は、認証されたユーザの銀行口座（個人データ管理部２１に保存されいる）から直接引き落とすことが可能である。

【００２７】個人認証部３１には、例えば、指紋によるユーザの認証を行う場合、指紋データベース３２により構成され、各ユーザの指紋に関するデータが保存される。

【００２８】図２は、端末１の外観の構成を示している。ディスプレイ５１は、電話番号、残量度数、個人情報などを表示する。受話器５２は、音声の送受信を行う際に用いられる。選択ボタン５３は、ディスプレイ５１に表示されている情報で良い場合に操作される「YES」ボタン、良く無い場合に操作される「NO」ボタン、次の情報を表示させたい場合に操作される「NEXT」ボタン、前の情報を再び表示させたい場合に操作される「PreV」ボタン、および直前の操作をキャンセルする際に操作される「キャンセル」ボタンから構成されている。指紋認識装置５４は、ユーザの認証を指紋により行う装置である。

【００２９】ダイヤルボタン５５は、「０」乃至「９」の１０のボタンと、２つの記号からなるボタンの、合計１２個のボタンから構成されており、電話番号の入力や、ディスプレイ５１上に表示されている情報の選択（後述）などを行う際に操作される。また、カード出入口５６は、端末１専用の料金前払い式のカード（テレフォンカード）や、個人認証用のカードが、挿入されたり、排出されたりするために設けられている。

【００３０】ユーザの認証の仕方は、指紋の他に、虹彩、顔の輪郭等の画像認識を用いる他、接触型のカードを用いるカード認識方式、ソニー（商標）のFelicaによる認証方式、携帯機器間の通信に人体を伝送媒体にするＰＡＮ（Personal Area Network）を用いた認証方式、手書きサインによる認証方式、または他の認証方式を用いることが可能である。また、これらの認証の仕方に応じたデータが、サーバ５の個人認証部３１に保存されている。さらに、これらの認証の仕方に応じた認証装置が、端末１の指紋認識装置５４の変わりに設けられる。例えば、認証にカードによる認識を用いる場合、指紋認識装置５４の変わりに、カードデータ読み出し装置を設ける（この場合、カード出入口５６に、データ読み出し機能を備えさせることも可能である）。また、ＰＡＮによる方式の場合、データを受信する受信装置、手書きのサインの場合、サインを入力するためのペンと画面（ディスプレイ５１で代用しても良い）を設ける。

【００３１】以下、個人認証用データとして指紋を用いる場合を例に挙げ、図３のフローチャートを参照して、端末１を用いて個人情報を取得する際の動作を説明する。

【００３２】ユーザは、ステップＳ１において、サーバ５とアクセスを開始する。まずユーザは、端末１にサーバ５にアクセスするための電話番号をダイヤルボタン５５を操作して入力する。その結果として、ネットワーク４を介して端末１とサーバ５は接続される。接続が完了

されると、そのことをユーザに知らせるために、端末１のディスプレイ５１上に、「接続が完了しました」、「指紋を入力して下さい」等の文字が表示される。ユーザは、ステップＳ２において、指紋認識装置５４に自分の親指を押しつけ、指紋の入力を行う。指紋認識装置５４は、入力された指紋をデジタイズする。デジタイズされた指紋データは、ステップＳ３において、サーバ５に送信される。

【００３３】送信された指紋データは、サーバ５のユーザ管理部１１により受信される。ユーザ管理部１１の個人認証部３１は、ステップＳ４において、指紋データベース３２を参照し、受信した指紋データが存在しているか否かを判断する。指紋データ３２には、指紋データとその指紋の持ち主の名前などが関連付けられて保存されている。受信した指紋データが、指紋データベース３２に存在していないと判断された場合、換言すると、受信した指紋データの認証ができなかった場合、ステップＳ５に進む。

【００３４】ステップＳ５において、認証に失敗した回数が３回目であるか否かが判断される。３回目であると判断された場合、不正なユーザとみなされ、通信は切断される。なお、この場合、認証に失敗した回数を３回としたが、他の回数に設定してもよい。また、不正なユーザとみなされた場合、通信を切断するのではなく、特定のデータベースにしか接続できないようにしても良い。

【００３５】一方、ステップＳ５において、認証に失敗した回数が３回以下であると判断された場合、ステップＳ６に進み、エラーメッセージが端末１に送信される。そのメッセージは、例えば、「もう一度指紋を入力して下さい」、「ユーザ確認に失敗しました」等である。ユーザは、このエラーメッセージに対応した処理として、ステップＳ２以下を繰り返す。

【００３６】一方、ステップＳ４において、送信された指紋データが指紋データベース３２に存在している（認証できた）場合、ステップＳ７に進み、情報の選択メニューを送信する。この選択メニューは、例えば図４に示した項目リスト７１のように表示される。この項目リスト７１は、認証されたユーザが、データ管理部１０に管理させているデータの項目などから構成されている。この表示例では、ユーザは、「スケジュール」，「住所録」，「預金残高」、および「顧客リスト」を個人データ管理部２１に保存させていることを示している。また、インターネットサービスは、システム内にインターネットへのゲートウェイとproxy機能を持たせることにより、ユーザが利用することが可能になる。

【００３７】項目リスト７１の「その他」は、上述した処理以外の処理を行いたい場合に選択される。上述した以外の処理とは、例えば、有料ソフトのダウンロード、他のユーザに伝言を伝送する、などである。また、「終了」は、これらの処理を終了させたい場合に選択される。

【００３８】コマンドボタン７２は、選択ボタン５３（図２）と対応している。ユーザは、このコマンドボタン７２を選択したい場合、選択ボタン５３の対応するボタンを操作すればよい。

【００３９】ユーザは、ステップＳ８において、表示された項目リスト７１の中から、所望の処理を選択する。ユーザは選択したい項目リスト７１の番号と同じ番号のダイヤルボタン５５を操作する。操作された番号の項目は、点滅させる、色を付けて表示させるなど、他の項目と区別がつく用に表示される。そして、ユーザは、その選択で良い場合には、コマンドボタン７２（選択ボタン５３）の「YES」ボタンを操作する。この選択された番号に対応する信号は、サーバ５に伝送される。サーバ５は、ステップＳ９において、伝送された信号は、終了を意味する信号であるか否かを判断する。終了を意味する信号であると判断された場合、端末１とサーバ５との接続は切られる。

【００４０】一方、サーバ５が、受信した信号は、終了を意味する信号でないと判断された場合、ステップＳ１０に進み、その信号に対応するデータをデータ管理部１０から読み出し、端末１に送信する。送信されたデータは、端末１のディスプレイ５１上に表示される。ユーザは、表示された画面から情報を得た後、ステップＳ８に戻り、さらに次の画面をみる、処理を終了させるなどの所望の処理を選択する。そして、ステップＳ８以降の処理が繰り返される。

【００４１】なお、上述した実施の形態においては、サーバ５に接続する際に、ユーザの認証を行ったが、サーバ５２接続した後、必要に応じてユーザの認証を行うようにしてもよい。例えば、ユーザが、サーバ５に接続した後、一般データ管理部２２に管理されているデータ、換言すればユーザの認証の必要のないデータを取得したい場合には、認証は必要ないので行わない。そして、ユーザが個人データ管理部２１に管理されているデータ、換言すればユーザの認証を必要とするデータを取得したい場合には、認証が行われる。

【００４２】ステップＳ７において、ディスプレイ５１に表示される選択メニューの特別な場合として、ユーザに電子メールや他のユーザからの伝言が送信（サーバ５に保存）されている場合、そのことを知らせるために、例えば、図５に示したようにメッセージ「伝言が届いています」を表示させるようにする。ユーザは、このメッセージに対応して、ステップＳ８において、選択ボタン５３（コマンドボタン７２）を操作して、その伝言または電子メールを読むか否かを決定する。ユーザは、その伝言または電子メールを読む場合には、選択ボタン５３の「YES」のボタンを操作し、読まない場合は、「ＮＯ」のボタンを操作する。その選択結果は、サーバ５に伝送される。

【００４３】サーバ５は、ステップＳ９において、選択されたのは終了か否かを判断する。終了でないと判断された場合、ステップＳ１０に進み、受信した選択結果に対応するデータを送信する。「YES」のボタンが操作された場合は、サーバ５に保存されている伝言または電子メールが送信され、ディスプレイ５１に表示される。「ＮＯ」のボタンが操作された場合は、図４に示した選択メニューの画面が表示される。

【００４４】なお、上述した説明においては、ディスプレイ５１に伝言を表示させるようにしたが、他のユーザがサーバ５に音声により伝言を保存していた場合には、受話器５２により、ユーザに伝えられる。

【００４５】次に、サーバ５のデータ管理部１０に保存されているユーザのスケジュール情報について説明する。スケジュール情報は、vCalender準拠のフォーマットで保存されており、他のユーザからの書き込みはできないようになされている。換言すれば、ユーザ管理部１１により、正規のユーザであると認証されたユーザのみが、スケジュールの読み出しと書き込みができるようになされている。

【００４６】またサーバ５には、ｖCard準拠のパーソナルデータで構成されるアドレス帳機能を持たすことが可能である。この機能により、そこに管理されているアドレス帳から、所望の電話番号を読み出すことが可能であり、さらにそのまま直接その電話番号に発信することが可能となり、もってユーザがアドレス帳を持ち歩いたり、電話番号を探すなどのわずらわしさから解放される。

【００４７】さらに、サーバ５には、ｖCard準拠のパーソナル情報管理機能により、売り上げ管理データ、商品データ、および在庫管理データなどをリンクさせて、保存しておくことも可能である。そして、これらのデータは、上述した個人データとは異なり、企業内に存在する複数のユーザが読み出したり、書き込んだりすることが可能なデータとする必要がある。

【００４８】なお、上述したｖCardとvCalenderは、Netscape（商標）やIBM（商標）などが中心となっているVersitという業界団体が標準化を進めている、「電子名詞」や「電子カレンダー」の規格である。この規格は、一般のPIM（Personal Information Manager）や、グループウェアでの使用を前提とされている。また、異機種間での相互参照を可能にするための拡張仕様として、IETF（Internet Engineering Tasl Force）で検討されている。ｖCard，vCalender、およびVersitについての詳細については、以下に示すインターネット上で公開されている。

http://www.imc.org/pdi/vcardwhite.htm　（ｖCard，ｖCalenderについて）

http://www.imc.org/pdi/　（Versitについて）

【００４９】また、上述した実施の形態においては、選択ボタン５３またはダイヤルボタン５５を操作して、ディスプレイ５１上に表示された情報を選択するようにしたが、ディスプレイ５１上にタッチタブレットなどを装着することにより、ディスプレイ５１上を触ることにより選択できるようにしても良い。

【００５０】上記各処理を行うコンピュータプログラムは、フロッピディスク、ＣＤ－ＲＯＭなどの記録媒体に記録し、これをユーザに配布することで提供したり、ネットワークなどの伝送媒体を介して提供し、ハードディスク、メモリなどに記憶させることで提供することができる。

【００５１】

【発明の効果】請求項１に記載の情報処理装置、請求項８に記載の情報処理方法、および請求項９に記載の提供媒体によれば、個人認証用データを入力し、情報を表示し、表示された情報を選択するようにしたので、個人認証をした後に、個人データが取得されることが可能になる。

【００５２】請求項１０に記載の情報処理装置、請求項１１に記載の情報処理方法、および請求項１３に記載の提供媒体によれば、個人を認証するためのデータを蓄積し、他の情報処理装置から送信された個人認証用データが、蓄積されているデータ内に存在するか否かを判断し、個人認証用データが存在していると判断された場合、アクセス可能となる個人データを蓄積するようにしたので、個人認証をした後に、個人データが取得されることが可能になる。

【００５３】請求項１３に記載の情報処理システム、請求項１４に記載の情報処理方法、および請求項１５に記載の提供媒体によれば、第１の情報処理装置は、個人認証用データを入力し、入力された個人認証用データを送信し、情報を表示し、表示された情報を選択し、第２の情報処理装置は、個人を認証するためのデータを蓄積し、第１の情報処理装置から送信された個人認証用データが、蓄積されているデータ内に存在するか否かを判断し、個人認証用データが存在していると判断された場合、アクセス可能となる個人データを蓄積し、個人データ蓄積手段に蓄積されているデータを、第１の情報処理装置に送信するようにしたので、個人認証をした後に、個人データが取得されることが可能になる。

【図面の簡単な説明】

【図１】本発明の情報処理システムの一実施の形態の構成を示す図である。

【図２】図１の端末の外観の構成を示す図である。

【図３】図１の情報処理システムが行う動作について説明するフローチャートである。

【図４】図３のステップＳ７において、ディスプレイ５１に表示される画面の一例を示す図である。

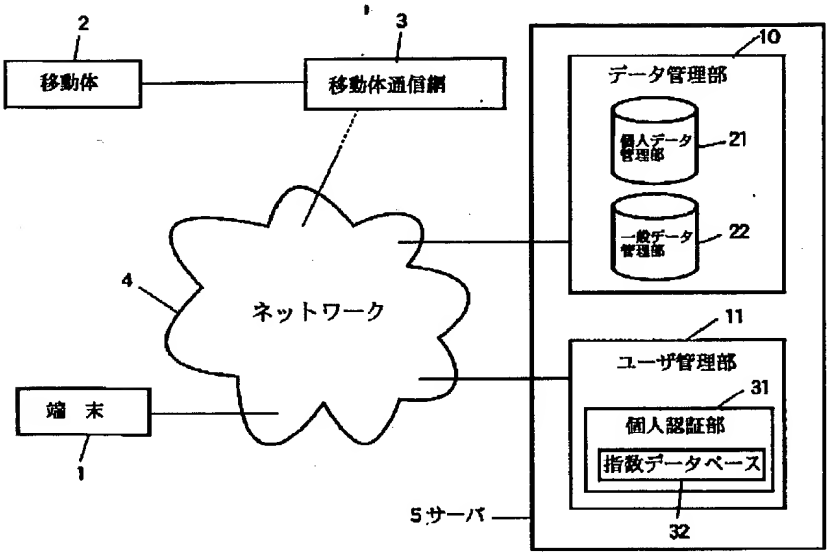
【図５】図３のステップＳ７において、ディスプレイ５１に表示される画面の他の例を示す図である。

13　　14

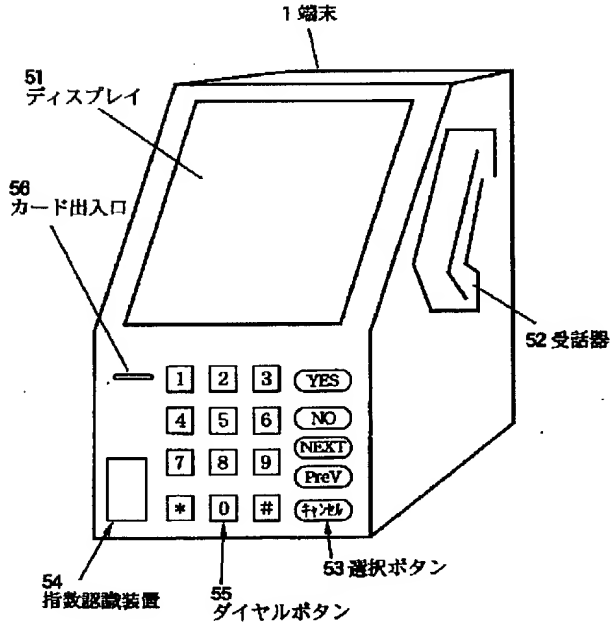
【符号の説明】

１　端末，　２　移動体，　３　移動体通信網，　４　ネットワーク，　５サーバ，　１０　データ管理部，　１１　ユーザ管理部，　２１　個人データ管理部，　２２　一般データ管理部，　３１　個人認証部，　３２　指紋データベース，　５１　ディスプレイ，　５２　受話器，　５３　選択ボタン，　５４指紋認識装置，　７１　項目リスト，　７２　コマンドボタン

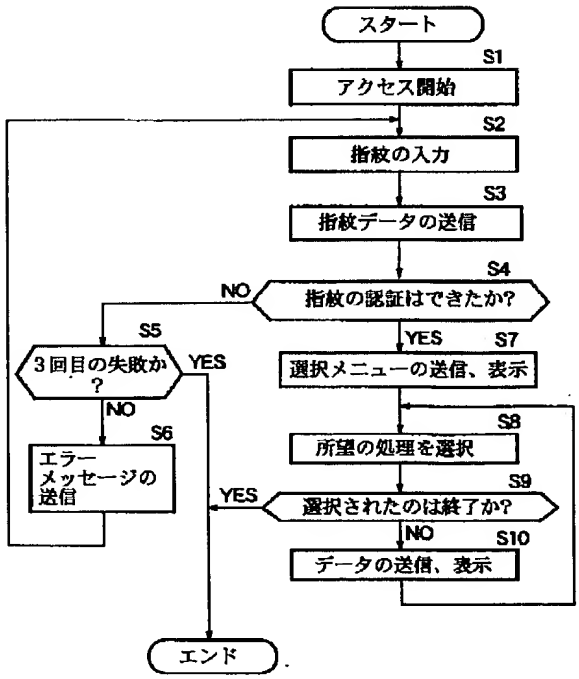
【図１】



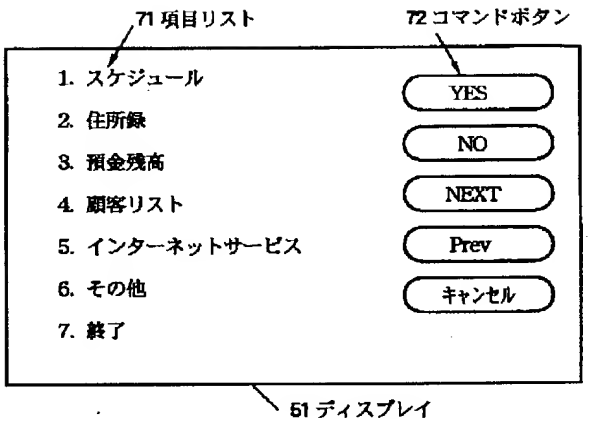
【図２】



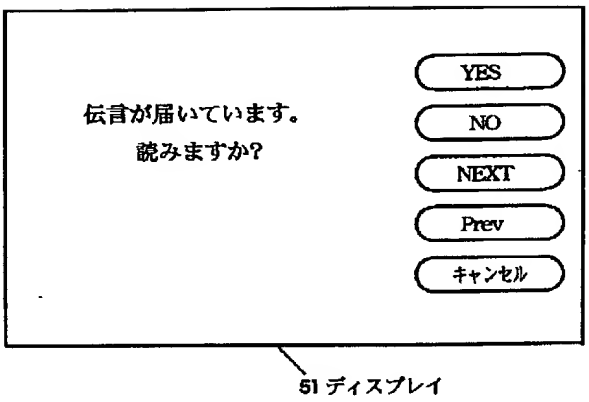
【図３】



【図４】


71 項目リスト
72 コマンドボタン
1. スケジュール
2. 住所録
3. 預金残高
4. 顧客リスト
5. インターネットサービス
6. その他
7. 終了
YES
NO
NEXT
Prev
キャンセル
51 ディスプレイ

【図５】


伝言が届いています。
読みますか?
YES
NO
NEXT
Prev
キャンセル
51 ディスプレイ